

Claims

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently amended) A method for compiling parser scripts each corresponding to the structure of security data received from a network component comprising ~~the steps of~~:
 - a) ~~identifying~~ sets of data categories, each set corresponding to security data received from one of a plurality of network components;
 - b) ~~constructing~~ database record definitions, each defining a record subdivided in accordance with one of the sets of data categories;
 - c) ~~writing~~ parser scripts that receive security data from the network components and output records, each record corresponding to one of the record definitions; and
 - d) ~~storing said parser scripts~~ in a data storage.
2. (Currently amended) The method of claim 1 further comprising ~~the steps of~~:
 - e) ~~determining~~ the format of each category in said sets; and
 - f) ~~formatting~~ the subdivisions to match the formats of the categories of the set to which the definition corresponds; [[and]]wherein each of the output records ~~of step (c)~~ correspond in format to one of the record definitions.
3. (Currently amended) The method of claim 1 further comprising ~~the steps of~~:
 - e) ~~building~~ database tables in a relational database each having the fields of one of the database record definitions; and
 - f) ~~inserting~~ output records received from the parser scripts into the tables.

4. (Currently amended) The method of claim 2 further comprising the steps of:
 - g)——building database tables in a relational database each having the fields and formats of one of the database record definitions; and
 - h)——inserting output records received from the parser scripts into the tables.
5. (Currently amended) The method of claim 1 wherein~~[[::]]~~ at least one of the sets of data categories is identified, ~~at least in part, from~~ by the product specifications of the network components.
6. (Currently amended) The method of claim 1 wherein~~[[::]]~~ at least one of the sets of data categories is identified, ~~at least in part,~~ by applying a Management Information Base (MIB) integrator to a Management Information Base for the corresponding network component.
7. (Currently amended) ~~An information network security data compilation system,~~ comprising:
 - a)——a first network component;
 - b)——a second network component;
a data storage element; and
 - e)——a data parser coupled to the first and second network components having access to a first parser script and a second parser script stored in the data storage element, the data parser is operable to produce categorized data from the data received from the first and second network components data interface operating with the first and second parser scripts, respectively.
8. (Currently amended) The ~~data compilation system~~ of claim 7 wherein: a) the first network component is a firewall and b)——the second network component is an intrusion detection system.

9. (Currently amended) The ~~data compilation~~ system of claim 7 further comprising:
a) —a third network component; and
b) —a distributed data manager; ~~[[and]]~~
wherein~~[[:]]~~ the data parser is coupled to the second and third network components through the distributed data manager, which collects and compresses data from the second and third network components and forwards the compressed data to the data parser.
10. (Currently amended) The ~~data compilation~~ system of claim 7 further comprising:
a) —a third network component;
b) —a second data parser coupled to the third component having access to a third parser script, the second data parser operable to produce categorized data from the data received from the third network component with the third parser script; and
c) —a relational database coupled to the first and second data parsers.
11. (Currently amended) The ~~data compilation~~ system of claim 7 further comprising:
a) —a display coupled to the data parser; and
b) —a relational database coupled between the data parser and the display;
~~and;~~
wherein~~[[:]]~~ the data parser transfers the categorized data to the relational database.
12. (Currently amended) The ~~data compilation~~ system of claim 11 wherein~~[[:]]~~ the relational database receives a data query and the display shows a portion of the categorized data, up to and including all the data~~[[,]]~~ from the relational database, corresponding to the data query.

13. (Currently amended) The ~~data compilation~~ system of claim 12 wherein~~[[:]]~~ the data queries are submitted through a web browser interface and the display shows the portions are shown through ~~[[a]]~~ the web browser interface.

14. (Currently amended) The ~~data compilation~~ system of claim 7 further comprising: a) an event detector coupled to the data parser, ~~and wherein~~~~[[:]]~~ the event detector compares the categorized data to a predetermined event definition and provides a signal that indicates that ~~[[if]]~~ a match is found between the categorized data and the predetermined event definition.

15. (Currently amended) The ~~data compilation~~ system of claim 7 further comprising: a) an information technology agent and wherein~~[[:]]~~ the network component is programmed by software, the agent collects security data from the software, and the data provided from the first network component is the security data collected by the agent.

16. (Currently amended) The ~~data compilation~~ system of claim 7 wherein~~[[:]]~~ data produced by the data parser produces is formatted and categorized data.

17. (Currently amended) The ~~data compilation~~ system of claim 7 wherein~~[[:]]~~ data from the first network component is security data and data from the second network component is security data.

18. (Currently amended) The ~~data compilation~~ system of claim 7 wherein~~[[:]]~~ data from the first network component is encrypted and decrypted.

19. (Currently amended) A method of compiling network security data comprising ~~the~~ steps of:

- a) —collecting security data from a plurality of network components;
- b) —accessing a plurality of different parser scripts, each script corresponding to one of the network components;
- c) —applying the plurality of different parser scripts to the security data to produce categorized and formatted data; and
- d) —storing the categorized and formatted data in a data storage.

20. (Currently amended) The method of claim 19 wherein~~[[::]]~~ the plurality of network components ~~includes at least~~ comprises a firewall and an intrusion detection system.

21. (Currently amended) The method of claim 19 further comprising the steps of:

- e) —transmitting the categorized and formatted data to a relational database;
- f) —providing a user interface for submitting queries to the relational database; and
- g) —displaying the categorized and formatted data, or a subset thereof, in accordance with submitted queries.

22. (Currently amended) The method of claim 21 wherein~~[[::]]~~ ~~step (e) transmitting~~ occurs prior to ~~step (d) storing~~ and ~~step (d) storing~~ comprises storing the categorized and formatted data in the relational database.

23. (Currently amended) The method of claim 19 further comprising the steps of:

- e) —comparing the categorized and formatted data to at least one predetermined event definition; and
- f) —generating a signal that indicates that ~~[[if]]~~ the data matches at least one event definition~~[[s]]~~.

24. (Currently amended) The method of claim 19 wherein one of the network components is programmed by software and an information technology agent communicates with the software to collect the security data.

25. (Currently amended) The method of claim 19 wherein the step of collecting occurs in real time rather than in batches.

26. (Currently amended) The method of claim 19 wherein at least two of the plurality of different data constructs correspond to the same network component.